Appendix C

Other information provided by the CA

The information included herein is presented by the management of MOE to provide additional information to users of this report. This information has not been subjected to the procedures of this engagement, and, accordingly, Deloitte Anjin express no opinion on it.

Comments on qualified opinion

	Observation	Additional MOE comments
1	The CA certificate, CA134100031, does NOT contain HTTP URLs in CRL Distribution Point extension. The CA certificate, CA134100031, does NOT have authorityInformationAcesss extension. This caused WebTrust Principles and Criteria for Certification Authorities – SSL Baseline with Network Security v2.3, Principle 2, Criterion 2.4 to not be met.	MOE has requested the issuance of a new subordinate CA certificate, including authorityInformationAccess extension and HTTP CRL information, from the Ministry of the Interior and Safety, the Root CA.
2	Validity period of some of subscriber certificates issued from 1 March 2018 exceeded the maximum that is 825 days. This caused WebTrust Principles and Criteria for Certification Authorities – SSL Baseline with Network Security v2.3, Principle 2, Criterion 2.7 to not be met.	During the period, five (5) certificates with a validity period of more than 825 days were issued. Subsequently, they were revoked and a patch to fix the bugs was implemented.
3	During the period, there were instances regarding DN structure with fixed values: • organizationName was fixed as Government of Korea; • organizationalUnitName was fixed as Group of Server; and • locallyName and stateOrProvinceName were not exist. Certificates which have multiple commonNames in Subject were issued. This caused WebTrust Principles and Criteria for Certification Authorities – SSL Baseline with Network Security v2.3, Principle 2, Criterion 2.14 to not be met.	A patch to fix the bugs was implemented on 4 May 2018. MOE CA has issued subscriber certificates which contained the new DN structure as follows. CN = <domain name>, OU = <department name>, O = <organization name>, L= <location name>, S = <state name>, C = kr
4	A certificate which had RSA 2024 bits module was issued. This caused WebTrust Principles and Criteria for Certification Authorities – SSL Baseline with Network Security v2.3, Principle 2, Criterion 2.16 to not be met.	During the period, one (1) certificate with RSA key modulus less than 2048 bits was issued. Subsequently, the certificate was revoked and a patch to fix the bugs was implemented.

	Observation	Additional MOE comments
5	During the period, validation of domain authorization was conducted by official documents classified as Domain Authorization Document. This caused WebTrust Principles and Criteria for Certification Authorities – SSL Baseline with Network Security v2.3, Principle 2, Criterion 4.1 to not be met.	A new process is currently being developed to provide domain validation that complies with the relevant SSL Baseline Requirements. According to the e-Government Act of Korea and the related laws, only government officials and school personnel are allowed to apply for a SSL certificate provided by MOE CA. An official document issued from the government authority and educational institute that has been checked using WHOIS data is acceptable as evidence of identity and domain validation according to Notification No.2018-152 of Ministry of Education.
6	Procedures on prevention by a CAA record were not documented. This caused WebTrust Principles and Criteria for Certification Authorities – SSL Baseline with Network Security v2.3, Principle 2, Criterion 4.11 to not be met.	Currently, government and schools don't use CAA records.
7	Some of subscriber certificates were not revoked within 24 hours after the CA recognized mis-issued certificates. This caused WebTrust Principles and Criteria for Certification Authorities – SSL Baseline with Network Security v2.3, Principle 2, Criterion 5.3 to not be met.	A new process has been developed to revoke mis-issued certificates within 24 hours after CA recognition.